This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of providing a ~~single sign-on~~ distributed application services integration, comprising the steps of:

providing a central domain server, wherein a configuration file resides on the central domain server, and the configuration file contains a list of cookie fields that may be read, or written to, and identifies whether a particular application has read access or write access, to a field of a cookie file;

receiving a first indication of a user pointing a browser to a first application;

receiving a cookie file of said browser corresponding to the user;

updating said cookie file;

receiving a second indication of said user pointing said browser to a second application; and

providing the second application with read access to different fields of the updated cookie file as determined by the list of cookie fields which identifies which cookie fields the second application has read access to, and providing the second application with write access to different fields of the cookie file as determined by the list of cookie fields which identifies the cookie filed that the second application has write access to. ~~said updated cookie file to said second application.~~

2. (currently amended) The method of claim 1 wherein said cookie file ~~of said server domain~~ received [[a]] at said receiving step is encrypted.

3. (original) The method of claim 2 further including the step of decrypting said encrypted cookie file.

4. (currently amended) The method of claim 1 wherein said cookie file is at most ~~approximately~~ 4 Kbytes.

5. (original) The method of claim 1 wherein said first and second applications each includes one or more predetermined resources.

6. (original) The method of claim 5 wherein said predetermined resources include one or more of a web page, a CGI script and a java servlet.

7. (original) The method of claim 1 wherein said first and second applications reside in a central server domain.

8. (original) The method of claim 1 wherein said first and second applications are third party applications residing in a central server domain.

9. (original) The method of claim 1 wherein said step of updating said cookie file includes the steps of:

comparing the cookie file to one or more of predetermined parameters; and

generating said updated cookie file based on said comparing step.

10. (original) The method of claim 9 wherein said step of comparing includes the step of reading said cookie file and retrieving a corresponding name=value pair for said user.

11. (original) The method of claim 9 wherein said predetermined parameters include a user identification information, a user event access history information, and a user access level information.

12. (original) The method of claim 11 wherein said user identification information includes one or more of a user name, a user social security number, a user address, a user telephone number, a user email address, a user age, a user gender, a user account type, and a user account activity history.

13. (original) The method of claim 1 wherein said step of providing said updated cookie file is performed synchronously with the step of receiving said second indication.

14. (currently amended) The method of claim 1 wherein when second indication of said user pointing said browser to a second application is received, fields of the updated cookie file are [[is]] automatically provided to said second application.

15. (original) The method of claim 1 wherein said first application resides in a central server, and further, wherein said second application is linked by a hypertext link to a remote site.

16. (original) The method of claim 1 wherein said step of receiving said first indication includes the steps of:

receiving a user login information; and

comparing said user login information to a predetermined login data.

17. (original) The method of claim 16 wherein said user login information includes a user name and a password.

18. (original) The method of claim 16 wherein said predetermined login data includes a user registration information.

19. (original) The method of claim 16 further including the step of permitting user browser access to said first application based on the outcome of the comparing step.

20. (original) The method of claim 19 wherein said user browser is permitted access said first application when said comparing step returns a match flag.

21. (original) The method of claim 19 wherein said user browser is not permitted access to said first application when said comparing step returns a fail flag.

22. (original) The method of claim 21 wherein when a fail flag is returned, said method further comprising the step of prompting said user to reenter the user login information.

Claims 23–37. (canceled)

38. (new) A method of providing a distributed application services integration system comprising:

providing a central domain server, wherein a configuration file resides on the central domain server, and the configuration file contains a list of cookie fields that may be read, or written to, and identifies whether a particular application has read access or write access, to a field of a cookie file;

providing a first application which transmits first application user event data to a first application interface library;

wherein the first application interface library determines whether the first application user event data is a first type of event data which requires a change to a field in a cookie file to provide real time communication to other applications of the system, and the first application determines whether the user event data is a second type of user event data which does not require real time communication to other applications of the system;

using a cookie access library to update a change in a field in the cookie file where the first application user event data is determined to be a first type of user event data;

where a first application user event data is determined to be a second type of user event data transmitting the user event data through message queuing middleware; and

controlling the first applications access to cookie fields of the cookie file based on the list in the configuration file.

39. (new) The method of claim 38 further including:

providing a second application which transmits a second application user event data to a second application interface library;

wherein the second application interface library determines whether the second application user event data is a first type of event data which requires a change to a field in the cookie file provide real time communication to other applications of the system, and the second application determines whether the second application user event data is a

second type of user event data which does not require real time communication to other applications of the system;

using a cookie access library to update a change a field in the cookie file where the second application user event data is determined to be the first type of user event data;

where a second application user event data is determined to be the second type of user event data transmitting the second application user event data through message queuing middleware; and

controlling the second applications access to cookie fields of the cookie file based on the list in the configuration file.

40. (new) The method of claim 38 further including:

encrypting first application user event data where the first application user event data is determined to be the second type of event data, prior to transmitting the first application user event data through the message queuing middleware.

41. (new) The method of claim 38 further including:

pushing information from the configuration file through the message delivering middleware to the first application interface library.

42. (new) The method of claim 41, wherein the information from the configuration file controls the operation of the first application interface library when a user event takes place.

43. (new) The method of claim 39 further including:

pushing information from the configuration file through the message delivering middleware to the first application interface library and the second application interface library.

44. (new) The method of claim 43, wherein the information pushed from the configuration file controls the operation of the first application interface library when a user event takes place, and controls the operation of the second application interface library